

## Hacked FTP site info

Contributed by John Nikolatos  
Tuesday, 09 January 2007

Client:

It appears that my ftp server may have been hacked. I am running Win 2K Server and in the inetpub/ftproot directory I have a folder called "." (Just a dot), but it says Access is denied even though I am the administrator.

When I run defrag it actually shows me the path of the files under the dot folder and here is what it shows:

```
\\inetpub\ftproot\.; . com1 . ; \Ratpack\filename
```

Is there anyway to get access to this folder so I can delete the directories?

Thanks,

NIKTEK:

please note - some data collected from the Internet.

If you read through this article it will explain how to HACKERS make hidden directories that are not easy to delete.

-BEGIN-

HACKER:

Many of you may have come with the problems that you have got some material or any thing personal which you don't wana share with any one, and afraid of being caught by your elder brother or by parents. so may place them in windows directory or may hide them but this is a very weak protection because any one having common sense will find for \*.jpg and from the names of the pics he or she can easily perceive that their is some thing wrong...many of my friends and many others have asked for a thousand time how to make it secure...so here is a very basic trick FOR THOSE WHO DON'T KNOW THIS. now first of all make a folder and name it any thing ( I prefer short

names because they are easy to use as g or f , I mean f is the name of folder). Now put all your personal material in that folder which u don't want to be shared.

Suppose you have make a folder in drive D and put all personal material in that folder now from start menu open MS-DOS prompt. change drive to D ( Don't ask me how to change the drive) Now we make use of a simple Debug command called move.

write  
 move [your folder name] Alt+any character in the "NUMPAD" (remember u have to use only NUMPAD , because it gives you an ASCII code) and then press enter.  
 mean it is  
 move[space] [your folder name][space]Alt+ur password.  
 be careful for spaces. when u will put Alt+password it will make an ASCII symbol. Now also be careful and use your common sense if the Alt+Numpad action makes an ASCII code if it doesn't then type any other number. Also it is advised that after doing this action go back to the location of the folder and check that if this technique has worked or not.  
 now I will show you by this figure.

```
C:\WINDOWS>D:
```

```
D:\>move f Ã
D:\f => D:\Ã [ok]
```

```
D:\>
```

this is the complete procedure. now when u will go to the D drive u wil see a folder and its name will be an underscore "\_".When u will try to open it it will display an error message

This folder 'D:\\_' doesn't exist what can you do with this folder.....

you can't do any thing with it ... you cant rename it, you cant delete it, you cant open it, you cant cut, copy, paste it to

any other location..

when you see of its properties it will show nothing .Of file size it will show 0 bytes (0 bytes) 0 bytes used...when created ..not known ..so this trick does a maximum security for your personal folder.

Now you think I have secured it but how to access it again...so now to do this again go to Ms DOS prompt and then type the command move Alt+your password f (the new folder name can be any its not necessarily to be the same old one from which you have moved it) so it is move[space]Alt+yourpassword[space]f

```
D:\>move Ã f
```

```
D:\Ã => D:f [ok]
```

```
D:\>
```

Now when u go back to that location u will find the folder f their and with all your material.

HERE IS SOME MORE INFO IF THAT DOES NOT WORK

How to Remove Files with Reserved Names in Windows

View products that this article applies to.

This article was previously published under Q120716

SUMMARY

Because programs control the policy for creating files in Windows, files sometimes are created by using names that are not valid or reserved names, such as LPT1 or PRN. This article describes how to delete such files by using the standard user interface.

#### MORE INFORMATION

NOTE: You must be logged on locally to the Windows computer to delete these files.

If the file was created on a file allocation table (FAT) partition, you may be able to delete it under MS-DOS by using standard command line utilities (such as DEL) with wildcard(s).

For example:

```
DEL PR?.*
```

-or-

```
DEL LPT?.*
```

These commands do not work on an NTFS file system partition as NTFS supports the POSIX subsystem and filenames such as PRN are valid under this subsystem. However, the operating system assumes the program that created them can also delete them; therefore, you can use commands native to the POSIX subsystem.

You can delete (unlink) these files using a simple, native POSIX program.

For example, the Windows Resource Kit includes such a tool, Rm.exe.

NOTE: POSIX commands are case sensitive. Drives and folders are referenced differently than in MS-DOS. Windows 2000 and later POSIX commands must use the following usage syntax:

posix /c <path\command> [<args>] IE: posix /c c:\rm.exe -d AUX.

Usage assumes Rm.exe is either in the path, or the current folder:

rm -d //driveletter/path using forward slashes/filename

For example, to remove a file or folder named COM1 (located at C:\Program Files\Subdir in this example), type the following command:

```
rm -d "//C/Program Files/Subdir/COM1"
```

To remove a folder and all of the its contents (C:\Program Files\BadFolder in this example), type the following command:

```
rm -r "//C/Program Files/BadFolder"
```

Another option is to use a syntax that bypasses the typical reserve-word checks completely.

For example, you can possibly delete any file with a command such as:

DEL \\.\driveletter:\path\filename

For example:

DEL \\.\c:\somedir\aux

If the name in the file system appears as a directory, use the following syntax.

For example, you can possibly delete any directory with a command such as:

RD \\.\<driveletter>:\<path>\<directory name>

For example:

RD \\.\c:\somedir\aux

-or-

Rmdir \\.\<driveletter>:\<path>\<directory>

For example:

Rmdir \\.\C:\YourFTP\_ROOT's\_PATH\COM1 /s /q

/s-This switch removes all directories and files in the specified directory and also the directory itself. This switch also removes a directory tree.

/q-This switch stands for Quiet mode. Do not ask if you can remove a directory tree that contains the /s switch.